Configurer SVM-scoped NDMP

ONTAP 9

NetApp
April 24, 2024

Sommaire

Configurer SVM-scoped NDMP

Activer SVM-scoped NDMP sur le cluster

Si le DMA prend en charge l'extension Cluster Aware Backup (CAB), vous pouvez sauvegarder tous les volumes hébergés sur différents nœuds d'un cluster en activant SVM-scoped NDMP, en activant le service NDMP sur le cluster (admin SVM) et en configurant les LIF de données et de contrôle.

Ce dont vous avez besoin

L'extension CAB doit être prise en charge par le DMA.

Description de la tâche

La désactivation du mode node-scoped NDMP permet d'activer le mode SVM-scoped NDMP sur le cluster.

Étapes

1. Activer le mode NDMP SVM-scoped :

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   Le mode NDMP SVM-scoped est activé.

2. Activer le service NDMP sur le SVM d'admin:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   Le type d'authentification est défini sur `challenge` par défaut, l'authentification en texte brut est désactivée.

   > Pour des communications sécurisées, vous devez maintenir l'authentification en texte brut désactivée.

3. Vérifier que le service NDMP est activé :

   ```
   cluster1::> vserver services ndmp show
   ```

   ```
   Vserver       Enabled   Authentication type
   ------------- --------- -------------------
   cluster1      true      challenge
   vs1           false     challenge
   ```

Activez un utilisateur de sauvegarde pour l'authentification NDMP

Pour authentifier SVM-scoped NDMP depuis l'application de backup, un utilisateur administratif doit disposer des privilèges suffisants et d'un mot de passe NDMP.

Description de la tâche

Vous devez générer un mot de passe NDMP pour les utilisateurs admin de sauvegarde. Vous pouvez activer les utilisateurs admin de sauvegarde au niveau du cluster ou de la SVM et, si nécessaire, vous pouvez créer un nouvel utilisateur. Par défaut, les utilisateurs disposant des rôles suivants peuvent s'authentifier pour la sauvegarde NDMP :

- Au niveau du cluster : `admin` ou `backup`
- SVM individuels : `vsadmin` ou `vsadmin-backup`

Si vous utilisez un utilisateur NIS ou LDAP, l'utilisateur doit exister sur le serveur respectif. Vous ne pouvez pas utiliser un utilisateur Active Directory.

Étapes

1. Afficher les utilisateurs et autorisations admin actuels :

   ```
   security login show
   ```

2. Si nécessaire, créez un nouvel utilisateur de sauvegarde NDMP avec le `security login create` Commande et le rôle approprié pour les privilèges des SVM au niveau du cluster ou individuels.

   Vous pouvez spécifier un nom d'utilisateur de sauvegarde locale ou un nom d'utilisateur NIS ou LDAP pour l' `-user-or-group-name` paramètre.

   La commande suivante crée l'utilisateur de sauvegarde `backup_admin1` avec le `backup` rôle pour l'ensemble du cluster :

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   La commande suivante crée l'utilisateur de sauvegarde `vsbackup_admin1` avec le `vsadmin-backup` Rôle d'un SVM individuel :

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Entrez un mot de passe pour le nouvel utilisateur et confirmez.

3. Générer un mot de passe pour la SVM d'admin via le `vserver services ndmp generate password` commande.

   Le mot de passe généré doit être utilisé pour authentifier la connexion NDMP par l'application de sauvegarde.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configurez les LIF

Vous devez identifier les LIF qui seront utilisées pour établir une connexion de données entre les données et les ressources sur bande, et pour contrôler la connexion entre la SVM d'administration et l'application de sauvegarde. Une fois les LIF définies, vous devez vérifier que les politiques de pare-feu et de basculement sont définies pour les LIF et spécifier le rôle d'interface privilégié.

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Étapes

1. Identifier les LIF intercluster, cluster-management et node-management en utilisant le `network interface show` commande avec `-role` paramètre.

   La commande suivante affiche les LIFs intercluster :

```
cluster1::> network interface show -role intercluster

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    IC1               up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2               up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   La commande suivante affiche la LIF cluster-management :

```
cluster1::> network interface show -role cluster-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    cluster_mgmt      up/up      192.0.2.60/24      cluster1-2
e0M     true
```

La commande suivante affiche les LIFs de node-management :

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------ ------------
------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24      cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24      cluster1-2
e0M     true
```

2. S’assurer que la politique de pare-feu est activée pour NDMP sur les LIF intercluster, cluster-management (cluster-mgmt) et node-management (node-mgmt) :

   a. Vérifiez que la politique de pare-feu est activée pour NDMP à l’aide de `system services firewall policy show` commande.

      La commande suivante affiche la politique de pare-feu pour la LIF cluster-management :

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                        ** ndmp       0.0.0.0/0**
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

La commande suivante affiche la politique de pare-feu pour la LIF node-management :

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Si la politique de pare-feu n'est pas activée, activez la politique de pare-feu à l'aide du `system services firewall policy modify` commande avec `-service` paramètre.

   La commande suivante active la politique de pare-feu pour le LIF intercluster :

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. S'assurer que la règle de basculement est correctement définie pour l'ensemble des LIFs :

   a. Vérifier que la policy de basculement pour la LIF de cluster-management est définie sur `broadcast-domain-wide`, Et la policy pour les LIFs intercluster et node-management est définie sur `local-only` à l'aide du `network interface show -failover` commande.

      La commande suivante affiche la politique de basculement pour les LIFs cluster-management, intercluster et node-management :

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ----------------- --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                     Failover Targets:
                                                     .......

**cluster1   cluster_mgmt       cluster1-1:e0m    broadcast-domain-wide
Default**
                                                     Failover Targets:
                                                     .......
           **IC1                 cluster1-1:e0a    local-only
Default**
                                                     Failover Targets:
           **IC2                 cluster1-1:e0b    local-only
Default**
                                                     Failover Targets:
                                                     .......
**cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
**cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
```

a. Si les stratégies de basculement ne sont pas définies de manière appropriée, modifiez la stratégie de basculement en utilisant le `network interface modify` commande avec `-failover-policy` paramètre.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Spécifier les LIFs requises pour la connexion de données à l'aide de `vserver services ndmp modify` commande avec `preferred-interface-role` paramètre.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vérifiez que le rôle d'interface préféré est défini pour le cluster à l'aide de `vserver services ndmp show` commande.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```